Scientific Research Publishing

Journal of Information Security, 2017, 8, 285-295
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Security and Privacy Challenges in Cyber-Physical Systems

Fahd AlDosari

Faculty of Computer and Information Systems, Umm AL-Qura University, Makkah, KSA
Email: fmdosari@uqu.edu.sa

How to cite this paper: AlDosari, F. (2017) Security and Privacy Challenges in Cyber-Physical Systems. *Journal of Information Security*, **8**, 285-295.
https://doi.org/10.4236/jis.2017.84019

Received: August 11, 2017
Accepted: October 10, 2017
Published: October 13, 2017

Abstract

Cyber-Physical Systems, or Smart-Embedded Systems, are co-engineered for the integration of physical, computational and networking resources. These resources are used to develop an efficient base for enhancing the quality of services in all areas of life and achieving a classier lifestyle in terms of a required service's functionality and timing. Cyber-Physical Systems (CPSs) complement the need to have smart products (e.g., homes, hospitals, airports, cities). In other words, regulate the three kinds of resources available: physical, computational, and networking. This regulation supports communication and interaction between the human word and digital word to find the required intelligence in all scopes of life, including Telecommunication, Power Generation and Distribution, and Manufacturing. Data Security is among the most important issues to be considered in recent technologies. Because Cyber-Physical Systems consist of interacting complex components and middle-ware, they face real challenges in being secure against cyber-attacks while functioning efficiently and without affecting or degrading their performance. This study gives a detailed description of CPSs, their challenges (including cyber-security attacks), characteristics, and related technologies. We also focus on the tradeoff between security and performance in CPS, and we present the most common Side Channel Attacks on the implementations of cryptographic algorithms (symmetric: AES and asymmetric: RSA) with the countermeasures against these attacks.

Keywords

Security, Cyber-Physical Systems, Side Channel Attacks

1. Introduction

1.1. What Are Cyber-Physical Systems?

Cyber-Physical Systems (CPS) are co-engineered embedded networked computing systems to compute, communicate and control natural or human-made systems [1]. The CPSs are integrated tightly together to provide high-level services (**Figure 1**).

In other words, Cyber-Physical Systems comprise several components and systems that are very different from each other, such as people, embedded systems, smart objects and physical environments. All parts are fused together through several network topologies and communication mediums, including the internet.

1.2. What Are the Key Features of Cyber-Physical Systems?

The Cyber-Physical systems are not only the interface between physical systems and computational systems, but they are also have all structural characteristics that emerge from combining two different kinds of systems, as shown in **Figure 2**. Some key features of CPS are [2]:

- All physical objects have a cyber capability that is IT-dominated.
- Every action is predicted in CPSs.
- Advanced sensing is applied to CPSs.
- All software and systems that are used are trusted and highly confident.
- CPSs always have one or more feedback loops from their output to their input.
- CPSs are self-documenting, self-monitoring and self-optimizing.
- CPSs should be securely connected via global networks.

1.3. What Are the Main Challenges of Cyber-Physical Systems?

Cyber-Physical Systems still face several barriers: scientific, technical, and social barriers. CPS technology integrates a significant number of heterogeneous physical objects and equipment with embedded and distributed systems that, together, must perform the required jobs efficiently and according to the performance specifications [3]. One of the biggest problems that such integrations face is the lack of consistent language and terminology that need to exist to describe cyber-physical interactions. However, there are no concrete foundations for a central interface among systems, physical objects and human, which makes the whole integration more difficult to be interoperable [3].

Human interaction with CPSs often encounter a critical challenge when interpreting the human-machine behavior and designing appropriate models that consider the current situational measurements and environmental changes. Such changes are crucial in the decision-making processes, particularly in systems such as air traffic systems and military systems [3]. Additionally, in sophisticated CPSs where suspicious activities must be handled immediately via machine learning approaches, outcomes and actions must not be surprising or uncertain. However, the existing procedures for defining suspicions are still insignificant, and there are software design errors, network connections and unreliable physical objects that exacerbate the problem [3].

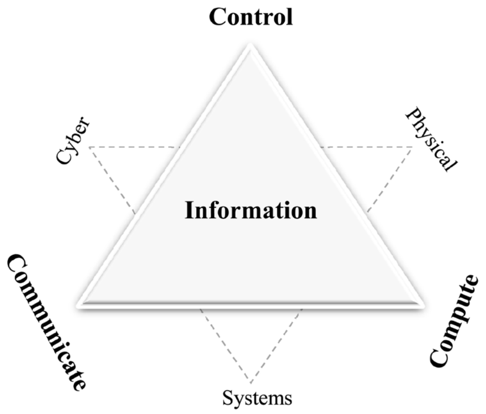

Figure 1. Cyber-physical system.

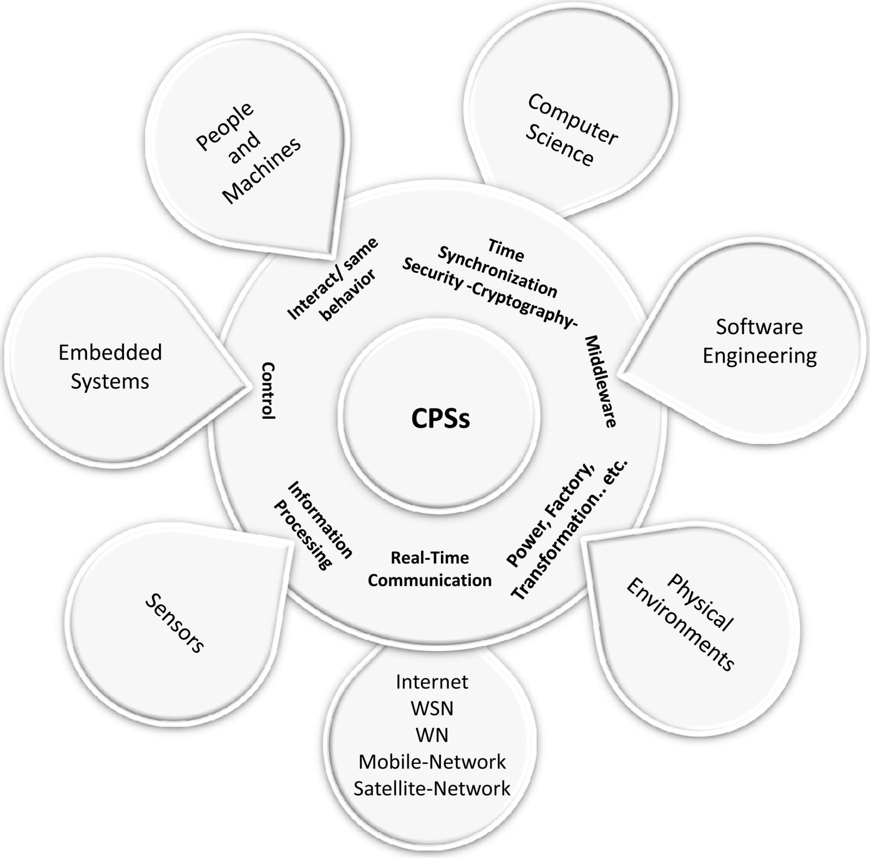

Figure 2. CPS and its parts and characteristics.

Moreover, there are challenges in maintaining the same required level of accuracy, reliability, and performance of all system parts, in addition to problems in the design phase of such systems, difficulties with compositionality and modularity for such systems and issues in dealing with the interdependencies between software and system engineering.

Security, privacy, and trust, as always, are the primary concerns for every modern technology. Keeping a CPS trustworthy and safe and protecting its private information from any possible manipulations are considered challenging problems both technically and politically. Security is ensured within several CPS levels, such as Infrastructure, individuals, intellectual property, and objects. Developing a security procedure to rapidly detect cyber and physical attacks and threats is challenging because there is a significant tradeoff between ensuring security and maintaining the required performance [4].

1.4. Security-Performance Tradeoff in CPS

According to most protection techniques for preserving sensitive data and information in CPSs, the optimal performance of the system must be detected by considering the privacy and security requirements. In other words, for each CPS, there is a particular compromise in which the required levels of security, privacy, and systems performance are all adjusted to obtain the best production and provide the best service.

CPSs are beneficial to many parts of life; they are susceptible to different kinds of attacks, depending on the dense communication between various IT objects through serried networks [4]. Thus, protecting a system's database from being accessed by unauthorized parties and preserving personal data and information from being exposed are critical challenges because implementing protection and encryption techniques to sensors is often infeasible due to a limited computational capacity [5].

The next section presents related work, followed by the security that should be achieved in Cyber Physical Systems environments in Section III. We discuss in Section IV Side Channel Attacks (SCA) on hardware implementations of symmetric and asymmetric encryption algorithms (AES and RSA) that are used to secure CPS. The countermeasures against these Side Channel Attacks are also presented.

2. Related Work

CPS technology was first presented to the president of the United States in 2011 because it had been listed as a top technical priority in networking and information technology research [6]. Since then, researchers have considered CPS-related technologies, challenges, and opportunities, and their designs and implementations are growing rapidly. In our paper, we focus on one aspect of a challenge facing this technology: the CPS security and security-performance trade-off. Ensuring secure communication and preventing untruthful data from spreading across a system is a critical concern because, as noted above, the existing protection techniques do not suit the particularity of this kind of system. In addition, severe losses may occur if no optimal compromise between security and performance is considered during CPS design. However, security in CPS is a hazardous issue: the efforts in considering it are still insufficient, and all of the studied solutions are mapped from current security techniques [6].

Here, we review some of the few types of research that discuss CPS security and the security-performance tradeoff. The authors of [7] propose an optimization for the security-performance tradeoff in CPS. They use the Co-evolutionary Genetic Algorithm (CGA) as a model, which returned efficient results for the optimization. The authors of [8] propose a framework to solve the contradiction between security and safety requirements and other CPS domain requirements such as performance. A performance-privacy optimization mechanism is proposed in [9] by using privacy requirements and a system's estimated cost. It is known that maintaining strong security without degrading the performance in any networked computing systems is a difficult task [10].

However, several research studies have discussed the security issue separately, with no consideration of the performance or the security-performance tradeoff. In [5], the authors discuss CPS security challenges and consider threats and possible attacks in addition to discussing specific properties that distinguish protection techniques of CPS from protection techniques of traditional IT systems. They also discuss the importance of developing new adversary models for CPS. In [11], the authors suggest a security design for CPS that considers specific common characteristics of CPSs, such as the CPS environment, real-time requirements, uncertainty and geographic distribution. Further, [11] indicates that taking care of security in CPSs should start at the very beginning of the designing phase by developing new appropriate security tools that meet the specific system requirements. In [12] the authors focus on being aware of the security issue, starting in the CPS design phase, by considering it to be the main part of the CPS developing process. They refer to three complementary approaches that help ensure security for such systems: approaches for securing multi-domain modeling and simulation, approaches to provide attack resiliency, and procedures to detect security challenges that affect the computing hardware of CPS.

The author of [13] surveys several symmetric and asymmetric LWC ciphers that are designed specifically for environments with hardware and software requirements. He selects hardware and software that had the latest implementations of several LWC ciphers and discusses both implementations for each cipher separately because specific characteristics can affect the hardware implementation but not the software implementation and vice versa. In [14], the authors provide several approaches to developing lightweight designs of traditional algorithms; they also highlight the main features that should be implemented in the algorithms and the main limitations that the algorithms should consider.

3. Safety and Security Objectives in CPS

1) Confidentiality is the ability to prevent information and data from being exposed to any unauthorized individual or party from inside or outside the system. Maintaining data and information confidentiality is done by applying encryption algorithms on stored and transmitted data and by restricting access to the places where data appear [15]. In CPS, Confidentiality is ensured by protecting communication channels from eavesdropping to prevent the system sta-

tus from being deduced, which may occur due to eavesdropping [16].

2) Integrity is the ability to keep data as it is and prevent any unauthorized manipulation. In other words, the data must be kept away from both outsiders and insiders who seek to modify it. Thus, a destination will receive incorrect data and treat it as correct. In CPS, Integrity is ensured by catching all possible attacks that seek to ruin the CPS's physical goals and change data that are collected and sent by sensors [17].

3) Availability: Generally, this is the system's ability to provide services and output products in a time manner. Availability is the ability of all subsystems to work properly and have their work done on time and when needed [18]. In other words, availability ensures that all CPS subsystems are functioning correctly by preventing all types of corruption, such as hardware and software failures, power failures and DoS attacks.

4) Authenticity: This is the ability to guarantee that all parties participating in any CPS processes are supposed to do so. Authenticity must be realized in all subsystems and processes to have an authentic and genuine CPS [15].

5) Robustness is the degree to which CPS can continue to work properly, even in the presence of limited disturbances. There are two types of failures: limited failures that have limited consequences and occasional failures whose little effects disappear with time [16].

6) Trustworthiness is the degree to which people (e.g., Owners, users, and individuals) can rely on the CPS to perform required tasks under specific domain constraints and according to specific time conditions [19]. The software, hardware, and collected data must all show level trustworthiness to consider a CPS feasible and trustworthy.

4. Side Channel Attacks: Differential Power Analysis Attack (DPA) on AES and RSA and the Countermeasures

The Side Channel Attacks (SCA) was introduced by Paul Kocher [20]. They exploit leaked Side Chanel information including energy consumption and execution time from the chips in the hardware implemented cryptosystems. The goal of the SCA is to reveal the secret keys and they can be applied to many running cryptographic devices including smart cards, mobile phones, RFID based systems, and CPS.

One of these SCAs is the Differential Power Analysis attack (DPA). It utilizes the inconstancy of power consumption to detect the secret information using statistical techniques. This inconstancy in power consumption is due to the different computations and operations being performed on the data. In this attack, there are two main techniques: data collection and data processing. In the following subsections we will present the DPA attacks and their countermeasures for the RSA and AES implementations.

For RSA implementations, the DPA attack on CRT-RSA focuses on the modular reduction performed prior to the modular exponentiations [21]. The attack performs correlation on series of power consumption traces of chosen RSA messages to find the prime. Another correlation attack that exploits the relation between consecutive modular squaring operations and modular multiplications was presented in [22].

The Comparative Power Analysis (CPA) assumes that an attacker can input user-defined message to RSA device, and can reveal the secret key by less power consumption traces than that required by DPA. Another attack using messages X (mod N) and −X (mod N) for modular exponentiations was presented in [23]. This attack was generalized in [24] by generating a collision using a message pair (Y , Z) which satisfies $Y\ \alpha \equiv Z^{\beta}$ (mod N) and detecting the collision between two power consumption traces at a certain location determined by α and β. In [25], another DPA attack is proposed (SAED) which stands for Subtraction Algorithm Analysis on Equidistant Data. This attack does not consider power signal changes in the used algorithms and avoid it because of their assumption that equidistant input leads to algorithms changings which affects the power signal. In this attack, subtraction event information are used to gain the secret needed information.

Countermeasures. One good solution to avoid these attacks is to propose efficient and low power cryptographic implementations for the encryption algorithms [26]. To disturb DPA and RPA/ZPA, Binary Expansion algorithm that has random initial point is used [27]. The work in [28] suggested to use message masking prior exponentiation with a random value (r) to prevent MESD and ZESD and use exponent masking to prevent SEMD. The exponentiation can be masked by the addition of random multiple of $\Phi(N)= (p - 1)(q - 1)$. i.e., $\hat{e} = e+ \Phi(N)$. The computation of modular exponentiation proceeds from the random starting point towards the MSB using the right-to-left binary exponentiation algorithm, returns to the starting point and then moves towards the LSB using the left-to-right binary exponentiation algorithm [29]. The authors in [30] presented a randomized window-scanning RSA scheme resistant to power analysis attacks, specifically to the CPA that uses different inputs to the same algorithm and analyze the power consumption traces. Even if the attacker was able to recover the bits, it will be difficult to put those key bits in the correct order.

For attacking AES hardware implementations, similar methods used for RSA can be applied but in different context. However, there are attacks which target certain countermeasures for AES. For example, the multi-round power analysis attack is built to breach the countermeasures that are stratified by block cipher algorithm [31]. On the other side, several countermeasures intended to beat off the power analysis attacks over AES such as random masking [32] and hardware balancing [33]. Different techniques have different characteristics and some known with their high cost in different terms such as hardware balancing techniques. The high cost of hardware techniques comes from the high power and area consumption rates due to complex modular arithmetic operations involved such as division and multiplication [34]. To reduce this cost, a balancing technique MUTE that uses the supplemental processor only when needed is proposed in [35]. This balancing technique executes parallel AES algorithms by using MPSoC (Multiprocessor System-on-Chip. One of the two processors is used for the original AES executing using the original secret key and the other processor is used to execute the modified AES.

Hardware solutions are also proposed as in [36] where only one switching event is performed at every one cycle by implying Dynamic Differential Logic circuits (DDL) that is known by SABL (Sense Amplifier Based Logic). Wave Dynamic Differential Logic (WDDL) is another hardware solution that depends on DDL [37]. Different than scalable hardware architectures [38], the authors in [39] proposed hardware current flattening architecture that used a flatten current feedback module (FCFM) and pipeline current flattening module (PCFM) at the level instruction to flatten current internally. The authors in [40] proposed a double-width single core that takes the original input and secret keys. The input key is duplicated and the secret key is reversed and then concatenated to the original key and finally executed with the modified double-width AES algorithm.

5. Conclusion

Cyber-Physical Systems have many useful applications in our daily life and in the industrial, manufacturing and military fields. CPSs face several critical challenges, including information security, privacy-related concerns and the tradeoff between security and performance. Due to the size specifications and constraints of CPSs as well as their resource utilization, the conventional information security approaches are not the best solutions for CPSs because they are resource-starving approaches and have massive requirements to provide an adequate level of security. In this paper, we presented an overview of Cyber-Physical Systems, their main characteristics, related technologies, and security concerns and attacks. We also presented one of the most common side Channel Attacks (Differential Power Analysis) on the implementations of symmetric cryptographic algorithms (AES) and asymmetric algorithms (RSA) with countermeasures against these attacks.

Acknowledgements

The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for the continuous support. This work was supported financially by the Deanship of Scientific Research at Umm Al-Qura University (Grant Code: 15-COM-3-1-0017).

References

[1] Al Faruque, M.A. and Ahourai, F. (2014) A Model-Based Design of Cyber-Physical Energy Systems. 2014 19*th Asia and South Pacific Design Automation Conference* (*ASP-DAC*), Singapore, 20-23 January 2014, 97-104. https://doi.org/10.1109/ASPDAC.2014.6742873

[2] Klesh, A.T., Cutler, J.W. and Atkins, E.M. (2012) Cyber-Physical Challenges for Space Systems. *Cyber-Physical Systems* (*ICCPS*), *2012 IEEE/ACM Third International Conference*, Beijing, 17-19 April 2012, 45-52. https://doi.org/10.1109/ICCPS.2012.13

[3] Sztipanovits, J., Ying, S., Cohen, I., Corman, D., Davis, J., Khurana, H., Mosterman, P.J., Prasad, V. and Stormo, L. (2012) Strategic R&D Opportunities for 21st Century Cyber-Physical Systems. Technical Report for Steering Committee for Foundation in Innovation for Cyber-Physical Systems: Chicago, IL, USA, 13 March 2012.

[4] Zhang, H., Shu, Y.C., Cheng, P. and Chen, J.M. (2016) Privacy and Performance Trade-Off in Cyber-Physical Systems. *IEEE Network*, **30**, 62-66. https://doi.org/10.1109/MNET.2016.7437026

[5] Tawalbeh, L.A. and Al-Haija, Q.A. (2011) Enhanced FPGA Implementations for Doubling Oriented and Jacobi-Quartics Elliptic Curves Cryptography. *Journal of Information Assurance and Security*, **6**, 167-175, Dynamic Publishers, Inc., USA.

[6] Marburger, J.H., Kvamme, E.F., Scalise, G. and Reed, D.A. (2007) Leadership under Challenge: Information Technology R&D in a Competitive World. An Assessment of the Federal Networking and Information Technology R&D Program. Executive Office of the President Washington DC President's Council of Advisors on Science and Technology.

[7] Wang, E.K., Ye, Y.M., Xu, X.F., Yiu, S.-M., Hui, L.C.K. and Chow, K.-P. (2010) Security Issues and Challenges for Cyber-Physical System. *Proceedings of the* 2010 *IEEE/ACM Int'l Conference on Green Computing and Communications* & *Int'l Conference on Cyber*, *Physical and Social Computing*, Hangzhou, 18-20 December 2010, 733-738. https://doi.org/10.1109/GreenCom-CPSCom.2010.36

[8] Zeng, W.T. and Chow, M.-Y. (2012) Optimal Tradeoff between Performance and Security in Networked Control Systems Based on Coevolutionary Algorithms. *IEEE Transactions on Industrial Electronics*, **59**, 3016-3025. https://doi.org/10.1109/TIE.2011.2178216

[9] Sun, M., Mohan, S., Sha, L. and Gunter, C. (2009) Addressing Safety and Security Contradictions in Cyber-Physical Systems. *Proceedings of the* 1*st Workshop on Future Directions in Cyber-Physical Systems Security* (*CPSSW'*09), Newark, NJ, July 2009, 1-5.

[10] Tawalbeh, L.A., Haddad, Y., Khamis, O., Aldosari, F. and Benkhelifa, E. (2015) Efficient Software-Based Mobile Cloud Computing Framework. *Cloud Engineering* (*IC2E*), 2015 *IEEE International Conference on IEEE*, 317-322.

[11] Al Faruque, M., Regazzoni, F. and Pajic, M. (2015) Design Methodologies for Securing Cyber-Physical Systems. *Proceedings of the* 10*th International Conference on Hardware*/*Software Codesign and System Synthesis*, Amsterdam, 4-9 October 2015, 30-36.

[12] Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A. and Uhsadel, L. (2007) A Survey of Lightweight-Cryptography Implementations. *IEEE Design & Test of Computers*, **24**, 522-533. https://doi.org/10.1109/MDT.2007.178

[13] Panasenko, S. and Smagin, S. (2011) Lightweight Cryptography: Underlying Principles and Approaches. *International Journal of Computer Theory and Engineering*, **3**, 516. https://doi.org/10.7763/IJCTE.2011.V3.360

[14] Song, H., Fink, G.A., Jeschke, S. and Rosner, G.L. (2017) Security and Privacy in Cyber-Physical Systems: Foundations and Application. Wiley Publisher, Hoboken, NJ, 243-281.

[15] Tawalbeh, L.A., Mowafi, M. and Aljoby, W. (2013) Use of Elliptic Curve Crypto-

graphy for Multimedia Encryption. *IET Information Security*, **7**, 67-74. https://doi.org/10.1049/iet-ifs.2012.0147

[16] Rungger, M. and Tabuada, P. (2013) A Notion of Robustness for Cyber-Physical Systems.

[17] Lo'ai, A.T., Mehmood, R., Benkhlifa, E. and Song, H. (2016) Mobile Cloud Computing Model and Big Data Analysis for Healthcare Applications. *IEEE Access*, **4**, 6171-6180. https://doi.org/10.1109/ACCESS.2016.2613278

[18] Tawalbeh, L.A., Haddad, Y., Khamis, O., Benkhelifa, E., Jararweh, Y. and AlDosari, F. (2016) Efficient and Secure Software-Defined Mobile Cloud Computing Infrastructure. *International Journal of High Performance Computing and Networking*, **9**, 328-341. https://doi.org/10.1504/IJHPCN.2016.077825

[19] Kocher, P.C. (1996) Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. *Proceedings of CRYPTO*, Santa Barbara, August 1996, 104-113. https://doi.org/10.1007/3-540-68697-5_9

[20] Boer, B.D., Lemke, K. and Wicke, G. (2003) A DPA Attack against the Modular Reduction within a CRT Implementation of RSA. *Proceedings Cryptographic Hardware and Embedded Systems*, 228-243.

[21] Boer, B., Lemke, K. and Wicke, G. (2011) Defeating RSA Multiply always and Message Blinding Countermeasure. *Proceedings Topics in Cryptology*, 77-88.

[22] Yen, S.-M., Lien, W.-C., Moon, S. and Ha, J. (2005) Power Analysis by Exploiting Chosen Message and Internal Collisions—Vulnerability of Checking Mechanism for RSA-Decryption. Progress in Cryptology, My Crypt, 183-195.

[23] Homma, N., Miyamoto, A., Aoki, T. and Satoh, A. (2010) Comparative Power Analysis of Modular Exponentiation Algorithms. *IEEE Transactions on Computers*, **59**, 795-807. https://doi.org/10.1109/TC.2009.176

[24] Jong-Yeon, P., Dong-Guk, H., Okyeon, Y. and JeongNyeo, K. (2014) An Improved Side Channel Attack using Event Information of Subtraction. *Journal of Network and Computer Applications*, **38**, 99-105.

[25] Kim, C., Ha, J., Moon, S., Yen, S.-M., Liena, W.-C. and Kim, S.-H. (2005) An Improved and Efficient Countermeasure against Power Analysis Attacks.

[26] Jararweh, Y., Tawalbeh, L.A., Tawalbeh, H. and Moh'd, A. (2013) 28 Nanometers FPGAs Support for High Throughput and Low Power Cryptographic Applications. *Journal of Advances in Information Technology*, **4**, 84-90.

[27] Messerges, T.S., Daddish, E.A. and Sloan, R.H. (1999) Investigations of Power Analysis Attacks on Smartcards. *Proceedings USENIX Workshop on Smartcard Technology*, Berkeley.

[28] Yen, S.-M. and Joye, M. (2000) Checking before Output May Not Be Enough against Fault-Based Cryptanalysis. *IEEE Transactions on Computers*, **49**, 967-970. https://doi.org/10.1109/12.869328

[29] Tawalbeh, L.A.A. and Sweidan, S. (2010) Hardware Design and Implementation of ElGamal Public-Key Cryptography Algorithm. *Information Security Journal: A Global Perspective*, **19**, 243-252.

[30] Lu, J., Pan, J. and den Hartog, J. (2010) Principles on the Security of AES against First and Second-Order Differential Power Analysis. *Proceedings 8th International Conference*, Beijing, 22-25 June 2010.

[31] Messerges, T.S. (2000) Securing the AES Finalists against Power Analysis Attacks. *7th International Workshop Proceedings Fast Software Encryption*, New York, 10-12 April 2000.

[32] Sokolov, D., Murphy, J., Bystrov, A. and Yakovlev, A. (2005) Design and Analysis of Dual-Rail Circuits for Security Applications. *IEEE Transactions Computers*, **54**, 449-460. https://doi.org/10.1109/TC.2005.61

[33] Fan, J., Gierlichs, B. and Vercauteren, F. (2011) To Infinity and Beyond: Combined Attack on (ECC) using Points of Low Order. *Proceedings Cryptographic Hardware and Embedded Systems*, Berlin.

[34] Tawalbeh, L.A.A. (2004) A Novel Unified Algorithm and Hardware Architecture for Integrated Modular Division and Multiplication in gf (p) and gf (2n) Suitable for Public-Key Cryptography. 1-52.

[35] Tiri, K., Akmal, M. and Verbauwhede, I. (2002) A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards. *Proceedings of the* 2002 *Solid-State Circuits Conference*.

[36] Tiri, K. and Verbauwhede, I. (2004) A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation. *Proceedings of the Conference on Design*, *Automation and Test in Europe*, Washington DC.

[37] Tiri, K. and Verbauwhede, I. (2006) A Digital Design Flow for Secure Integrated Circuits. *Computer-Aided Design of Integrated Circuits and Systems*, **25**, 1197-1208. https://doi.org/10.1109/TCAD.2005.855939

[38] Tawalbeh, L.A., Tenca, A., Park, S. and Koc, C. (2005) An Efficient Hardware Architecture of a Scalable Elliptic Curve Crypto-Processor over GF (2n). *Optics and Photonics*, **59**, 100-105.

[39] Radu, M. and Gebotys, C. (2004) Current Flattening in Software and Hardware for Security Applications. Hardware/Software Codesign and System Synthesis, CODES + ISSS, 218-223.

[40] Arora, A., Ambrose, J.A., Peddersen, J. and Parameswaran, S. (2013) A Double-Width Algorithmic Balancing to Prevent Power Analysis Side Channel Attacks in AES. *IEEE Computer Society Annual Symposium on VLSI*, Natal, 5-7 August 2013, 76-83.